UNIVERSITI TEKNOLOGI MARA

WINDOWS REGISTRY ANALYSIS FOR FORENSIC PURPOSE

RIZIANA BINTI IBRAHIM

Dissertation submitted in partial fulfillment of the requirements for the degree of

Master of Science (Information Technology)

Faculty of Computer and Mathematical Sciences

July 2012

STUDENT'S DECLARATION

I declare that the work in this report was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the result of my own work, unless otherwise indicated or acknowledged as reference work. This report has not been submitted to any other academic institution or non-academic institution for any other degree or qualification.

In the event that my report be found to violate the conditions mentioned above, I voluntarily waive the right of conferment of my degree and degree to be subjected to the disciplinary rules and regulations of Universiti Teknologi MARA.

Name of Student Riziana binti Ibrahim
Student's ID No. 840518-02-5678 / 2009374447
Program Master of Science (Information Technology)
Faculty Faculty of Computer and Mathematical Sciences
Project Title Windows Registry Analysis for Forensic Purpose

Signature of Candidate
Date 31st July 2012

ABSTRACT

The cyber attack is a severe attack that might cause harm especially to the big organization. It is therefore the attacks need to be fight and stop. The attack comes in various approach and forms. One of it is through the channel of remote access. Many organizations nowadays had allowed the remote access due to the flexibility of their staffs working from home. Without conscious on the vulnerability, this organization continues to be susceptible to attack. Attacks can be initiated either by insider or outsider. The insider of course will have much more advantage assuming that they already know the organization's structure and passwords to the machine. One of the attacks that are top to be planted on the machine is spyware. This spyware is very useful to the attacker and very harmful to the machine's owner. In the event of an attack, an investigation must be carried out. The main purpose of investigation is to inspect the illegal activities and to get the potential evidence. In this study, Windows registry analysis was made on the Windows 7 Home Enterprise (32 bit) platform. The study was focused to identify the existence of unwanted application of the Virtual Network Computing (VNC) and keylogger application. The outcome of this study is the artifacts of the registry values in correlation to the user activities.

ACKNOWLEDGEMENTS

BISMILLAHHIRAHMANIRRAHIM

In the name of Allah, The Most Gracious and The Most Merciful. All praise belongs to Allah, Lord of the Universe. There is no god but Allah and Muhammad is his messenger, peace upon him.

First and foremost, praise is due to Allah the Almighty for His wisdom and blessings in giving me the strength and endurance in completing the project. I wish to thank various people for the parts they played in making this thesis possible. To begin with, I would like to express my deepest gratitude and sincere appreciation to my supervisor, Mrs. Rozita Binti Yunos, for her precious time, invaluable guidance, suggestions, comments, support and encouragement. She has inspired and empowered me greatly in my work. Besides, I wish to thank to my thesis coordinator, Dr. Fariza Hanis Binti Abdul Razak and also to all my lecturers Prof. Dr. Nor Laila Binti Md Noor, Dr. Wan Abdul Rahim Bin Wan Mohd Isa, Dr Kamarularifin Bin Abd Jalil, Dr. Wan Adilah Binti Wan Adnan, Dr. Ariza Binti Nordin and Assoc. Prof. Kalsom Binti Nasir.

I would also like to thank Mrs. Sarah Khadijah Taylor, the Head of the R&D Unit of Digital Forensics Department (DFD) at CyberSecurity Malaysia who are contributing the ideas and efforts on sharing information and furthermore to my graduate friends for the priceless support and contributions in making this thesis a success.

Finally, I wish to thank my beloved parents, Ibrahim Bin Md. Isa and Rihan Binti Hj. Awang for their heartening support, unconditional love and continuous prayer for me.

TABLE OF CONTENTS